SURVEY ON WIRELESS SENSOR NETWORKS

Vishnu.V,
B.Sc(Information Technology),
Department of Computer Science,
Sri Krishna Adithya College of Arts And Science,
Coimbatore-641042,Tamil Nadu,India.

Shyam Richard.S,
B.Sc(Information Technology),
Department of Computer Science,
Sri Krishna Adithya College of Arts And Science,
Coimbatore-641042,Tamil Nadu,India.

Abstract: In the past days of technology world, people can only able to link the computer devices with simple networking technology in order to perform technical activities and share resources. These can be created using several methods such as switches, routers cables, radio waves and beams. Later the technology developed into sensor networks. A Sensor network system consist of large number of sensor nodes with low power can be an effective tool for collection and integration of each sensor in a variety of areas. Now it's being an extreme level of networking technology. The Wireless Sensor Networks came into introduction. WSN'S is a wireless networking technology consisting of autonomous devices to perform the monitoring and functioning of the environments. In this paper we mainly emphasis on the WSN and its applications, recent technologies, future enhancement of WSN.

Keywords: Wireless Sensor Network, nodes, zig bee, ad hoc network

I. INTRODUCTION

Wireless Sensor Network (WSN) is one kind of wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called nodes. These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of computing & processing. Nodes are the tiny computers, which work jointly to form the networks. WSN's are collections of compact-size relatively inexpensive computational nodes measure local environmental conditions or other parameters and forward such to a central point for appropriate processing. WSNs nodes (WNs) can communicate with neighboring nodes, and can perform basic computations on the data being collected. WSNs support a range of useful applications. Wireless sensor networks (WSNs) have recently attracted a lot of interest in the research community due their wide range of applications. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to security threats that can adversely affect their proper functioning.

II.BACKGROUND STUDY

Wireless sensor networks are deployed on land, underground, underwater. A sensor network faces different challenges and according to the environment in the sensor networks. There are five types of the wireless sensor network as by Jennifer Yuck [1].

1.Terrestrial Wireless sensor network.2. Underground Wireless sensor network.3.Underwater Wireless sensor network.4.Multi-media Wireless sensor network.5.Mobile Wireless sensor network.

A Wireless sensor network (WSN) consists of wireless sensor nodes or motes, which are devices equipped with a processor, a radio interface, an analog-to digital converter, sensors, memory and a power supply. The processor provides the mote management functions and performs data processing. The sensors attached to the mote are capable of sensing temperature, humidity, light, etc. Due to bandwidth and power constraints, motes primarily support low data units with limited computational power and a limited sensing rate. Memory is used to store programs (instructions executed by the processor) and data (raw and processed sensor measurements). Motes are equipped with a low-rate (10- 100 kbps) and short-range (less than 100m) wireless radio, e.g., IEEE 802.15.4 radio to communicate among themselves. Since radio communication consumes most of the power, the radio must incorporate energy-efficient communication techniques.

The power source commonly used is rechargeable batteries. Since motes can be deployed in remote and hostile environments they must use little power and must employ built-in mechanisms to extend network lifetime. For example, motes may be equipped with effective power harvesting methods, such as solar cells, so they may be left unattended for years. Sensor nodes can be deployed in an ad-hoc or a pre-planned manner. An ad-hoc deployment is good for large uncovered regions where a network of a very large number of nodes can be deployed and left unattended to perform monitoring and reporting functions. Network maintenance such as managing connectivity and detecting failures is difficult in such a WSN due to large number of nodes. On the other hand, pre-planned deployment is good for limited coverage where fewer nodes are deployed at specific locations with the advantage of lower network maintenance and management cost.

UNIQUE FEATURES OF WSN: CHALLENGES AND REQUIREMENTS

The collaborative nature of WSNs brings several advantages over conventional wireless ad-hoc networks, including self-organization, rapid deployment, flexibility, and inherent intelligent-processing capability. However, the unique features of WSN present new challenges in hardware design, communication protocols, and application design. A WSN technology must address these challenges to realize the numerous envisioned applications. This requires modifying legacy protocols for conventional wireless ad-hoc networks or designing new effective communication protocols and algorithms [2].

Table 1 lists important challenges and corresponding required mechanisms to address them in WSN. Sensor nodes have resource constraints including limited energy, limited memory and computational capacities. The limited energy supplies of the sensor nodes in the network impose lifetime constraints on the WSN. The problem of limited resources can be addressed by using them efficiently. Energy efficient operation is required to maximize the network lifetime by implementing energy efficient protocols, e.g., energy-aware routing on network layer, energy-saving mode on MAC layer, etc. Efficient use of limited memory in sensors is required by taking into account the memory consuming issues like routing tables, data replication, security, etc.

Table 1 Challenges vs. Required mechanisms in WSN.

Challenges	Required mechanisms
Resource constraints	Efficient use of resources
Dynamic and extreme environment conditions	Adaptive network operation
Data redundancy	Data fusion and localized processing
Unreliable wireless communication	Reliability
No global identification (ID) for sensor nodes	Data-centric communication paradigm
Prone to node failures	Fault tolerance
Large scale deployment	Low-cost small-sized sensors with self-configuration and self-organization

Dynamic network topologies and harsh environment conditions may cause sensor-node failures and performance degradation. This requires WSN to support adaptive network operation including adaptive signal-processing algorithms and communication protocols to enable end-users to cope with dynamic wireless-channel conditions and varying connectivity. The communication in WSN is unreliable due to error prone wireless medium with high bit error rates and variable-link capacity. Thus, a WSN should be reliable in order to function properly and depending on the application requirements, the sensed data should be reliably delivered to the sink node. WSNs are usually prone to unexpected node failures due to different reasons like nodes may run out of energy or might be damaged (in extreme environment conditions), or wireless communication between two nodes can be permanently interrupted. This requires WSNs to be robust to node failures. In WSN, fault tolerance can be improved through a high level of redundancy by deploying additional nodes than required if all nodes functioned properly. In case of high density deployment, sensor observations can be highly correlated in the space domain. Data fusion and localized processing are required to address the data redundancy such that only necessary information is delivered to the end-user and communication overhead can be reduced. Since WSNs may contain a large number of sensor nodes, the employed architectures and protocols must be able to scale to sizes of thousands or more. Moreover, a large scale deployment of WSN requires low-cost and small-sized sensor nodes. A WSN should be able to self-organize itself as the network topology may change due to reasons like node failure, mobility, and large scale deployments. In addition, new nodes may need to join the network, for example, to replace failed nodes, thus, a WSN must be self-reconfiguring. It can be expensive to give a unique address for each node (address-centric paradigm) especially when thousands of nodes are deployed in the application. Global identification for sensors in a WSN lead to large overhead. Moreover, due to limited memory and computational power it is not advisable to depend on a single sensor node's contents. Thus, WSNs are required to use the data-centric paradigm which focuses on data generated by a group of sensors.

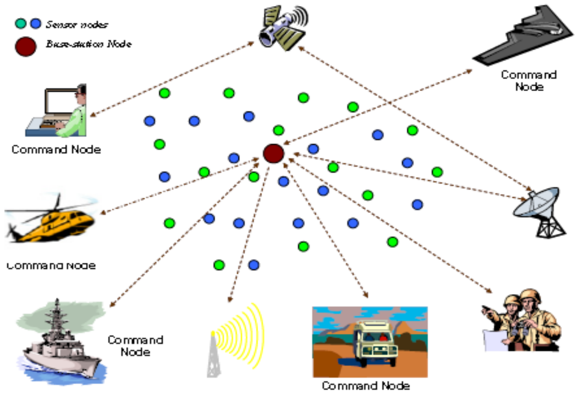

Fig. 1. A sensor network for a combat filed surveillance application. The base-station is deployed in the vicinity of the sensors to interface the network to remote command centers.

[3,4] Recent years have witnessed an increased interest in the use of wireless sensor networks (WSNs) in numerous applications such as forest monitoring, disaster management, space exploration, factory automation, secure installation, border protection, and battlefield surveillance. In these applications, miniaturized sensor nodes are deployed to operate autonomously in unattended environments. In addition to the ability to probe its surroundings, each sensor has an onboard radio to be used for sending the collected data to a base-station either directly or over a multi-hop path. Fig. 1 depicts a typical sensor network architecture. For many setups, it is envisioned that WSNs will consist of hundreds of nodes that operate on small batteries. A sensor stops working when it runs out of energy and thus a WSN may be structurally damaged if many sensors exhaust their onboard energy supply. Therefore, WSNs should be carefully managed in order to meet applications' requirements while conserving energy.

The bulk of the research on WSNs has focused on the effective support of the functional, such as data latency, and the non-functional, such as data integrity, requirements while coping with the resource constraints and on the conservation of available energy in order to prolong the life of the network. Contemporary design schemes for WSNs pursue optimization at the various layers of the communication protocol stack. Popular optimization techniques at the network layer include multihop route setup, in network data aggregation and hierarchical network topology [5]. In the medium access control layer, collision avoidance, output power control, and minimizing idle listening time of radio receivers are a sample of the proposed schemes [3,5]. At the application layer, examples include adaptive activation of nodes, lightweight data authentication and encryption, load balancing and query optimization. [6,7]

[8]ZigBee Alliance, Bishop Ranch, ZigBee based wireless networks are designed with different characteristics to WIFI. They are particularly suitable for so called machine-to-machine (M2M) applications. Consequently, ZigBee will be important in the powerful 'internet of things' that promises big changes to many aspects of life, and therefore business, through the hugely important 'second economy'. There are an increasing number of ZigBee based products so the name will pass into common parlance along with Wi-Fi as its inclusion in products becomes a marketing feature. It is important for the progressive business to take advantage of the new opportunities that ZigBee creates.

III.CONCLUSION

Wireless sensor networks (WSNs) have attracted lots of attention in recent years due to their potential in many applications such as border protection and combat field surveillance. The development of WSN will also generate to the next level. The future WSN's will be a smart working technology. The applications like video and underwater surveillance raise a number of interesting node placement challenges. Finally, we expect domain and node-specific positioning to gain increased attention with the growing list of WSN applications and the availability of sophisticated models of the capabilities of sensor nodes.

IV. FUTURE ENHANCEMENT

This scheme had provided improvement gains in Energy efficiency, Throughput, Delay, Bandwidth and deliver ratio. But the superior nature of this scheme depends on many environmental factors, such as operation scenarios, specific data types etc. Thus, more research work needs to be done in future to find the respective application scenarios for this scheme with all the related factors taken into consideration. This technique needs to be implemented in a wireless sensor network with mobile nodes, since mobility was not taken into account in this work. The effects of very large node densities need to be investigated. Multi hop routing was adopted in this work. The feasibility of using the clustering technique and data aggregation needs to be tested in the same wireless sensor network.

V. REFRENCES

[1] Jennifer Yuck, Viswanath Mukherjee, Dipak Ghoshal, "wireless sensor network survey," Computer Networks 52 (2008) 2292–2330.

[2] H. Karl, A. Willig, Protocols and architectures for wireless sensor networks, WileyInterscience, 2007.

[3] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks 38 (2002) 393–422.

[4] C-Y. Chong, S.P. Kumar, Sensor networks: evolution, opportunities, and challenges, Proceedings of the IEEE 91 (8) (2003) 1247–1256.

[3] K. Akkaya, M. Younis, A survey on routing protocols for wireless sensor networks, Elsevier Journal of Ad Hoc Networks 3 (3) (2005) 325–349.

[4] P. Naik, K.M. Sivalingam, A survey of MAC protocols for sensor networks, in: C.S. Raghavendra, K.M. Sivalingam, T. Znati (Eds.), Wireless Sensor Networks, Kluwer Academic Publishers, Norwell, MA, 2005, pp. 93–107.

[6] N. Sadagopan, B. Krishnamachari, A. Helmy, Active query forwarding in sensor networks (ACQUIRE), Journal of Ad Hoc Networks 3 (1) (2005) 91–113.

[7] A. Cerpa, D. Estrin, ASCENT: Adaptive self-configuring sensor networks topologies, in: Proceedings of the 21st International Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'02), New York, NY, June 2002.

[8] ZigBee Alliance, Bishop Ranch, CA, http://www.zigbee.org/.

[9] G.J. Pottie and W.J. Kaiser, Wireless integrated network sensors, Commun. ACM 43(5) (2000) 51–58.

[10] K. Sohrabi, J. Gao, V. Ailawadhi and G.J. Pottie, Protocols for selfo rganization of a wireless sensor network, IEEE Personal Commun. 7(5)(2000) 16－27.

[11] P. Bahl and V.N. Padmanabhan, RADAR: an in-building RF-based user location and tracking system, in: IEEE INFOCOM (2000) pp. 775–784

[12] D. Braginsky and D. Estrin, Rumor routing algorithm for sensor networks, in: ACM Int'l Workshop on Wireless Sensor Networks and Applications (WSNA) (2002).

[14] N. Bulusu, J. Heidemann and D. Estrin, GPS-less low cost outdoor localization for very small devices, IEEE Personal Commun. 7(5) (2000) 28–34.

[15] D. Ganesan, R. Govindan, S. Shenker and D. Estrin, Highly resilient, energy efficient multipath routing in wireless sensor networks, ACM Mobile Comput. and Commun. Review 5(4) (2001) 11－25.